Cyber Crime Volunteer Program

The Union Home Ministry has launched a Cyber Crime Volunteers Concept as a measure to fight cybercrime. In this article, you can read all about this concept, its particulars, and the associated concerns, from the perspective of the IAS exam.

Cyber Crime Volunteers Concept

In February 2021, the Ministry of Home Affairs flagged off the Cyber Crime Volunteers Program under the Indian Cyber Crime Coordination Centre (I4C) in a bid to fight cybercrime.

- The program tries to get citizens of the country involved in the process of fighting cybercrime.
- Under this program, citizens can register on the cybercrime volunteers program portal and flag unlawful content on the internet.
- These registered persons can help law enforcement agencies in identifying, reporting and removal of illegal or unlawful online content.
- Unlawful content under the program is defined as any content that can come under the following categories:
    - Against sovereignty and integrity of India
    - Against defence of India
    - Against security of the state
    - Against friendly relations with foreign states
    - Content aimed at disturbing public order
    - Disturbing communal harmony
    - Child sex abuse material
- There are two options for reporting cybercrimes on the portal:
    - Report crime related to women/children – Under this section, people can report complaints pertaining to online Child Pornography (CP), Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content. A complaint filed under this section cannot be withdrawn.
    - Report other cybercrimes – Under this option, registered citizens can report complaints pertaining to cybercrimes such as mobile crimes, online and social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber trafficking. A complaint made under this section can be withdrawn before it is converted into a First Information Report (FIR).
- Citizens providing false information can be charged under relevant sections of the Indian Penal Code (IPC).
- The program aims to enlist about 500 citizens to participate in the voluntary cyber crime-fighting program.

- Any citizen can register himself/herself under one of three categories: ‘Cyber Volunteer Unlawful Content Flagger’, ‘Cyber Awareness Promoter’, and ‘Cyber Expert’.

Indian Cyber Crime Coordination Centre (I4C)

I4C has been established as a nodal agency by the Ministry of Home Affairs to fight against cybercrime. It aims to provide a platform to deal with cybercrimes in a coordinated and comprehensive manner. One of the major goals of I4C is to create an ecosystem that brings together academia, industry, public and government in the prevention, detection, investigation and prosecution of cybercrimes.

I4C Objectives:

1. To identify the research problems/needs of law enforcement agencies and take up R&D activities in developing new technologies and forensic tools in collaboration with academia/research institutes within India and abroad.
2. To prevent the misuse of cyberspace for furthering the cause of extremist and terrorist groups.
3. To suggest amendments, if required, in cyber laws to keep pace with fast-changing technologies and international cooperation.
4. To coordinate all activities related to the implementation of Mutual Legal Assistance Treaties (MLAT) with other countries related to cybercrimes in consultation with the concerned nodal authority in the Home Affairs Ministry.

Components of I4C:

1. National Cybercrime Threat Analytics Unit (TAU)
2. National Cybercrime Reporting
3. Platform for Joint Cybercrime Investigation Team
4. National Cybercrime Forensic Laboratory (NCFL) Ecosystem
5. National Cybercrime Training Centre (NCTC)
6. Cybercrime Ecosystem Management Unit
7. National Cyber Crime Research and Innovation Centre

Cyber Crime Volunteers Concept Concerns

Some of the concerns expressed by experts on the scheme are mentioned below.

- There is no prior verification to be carried out for volunteers who want to sign up under the first category, whereas some form of authentication (know your customer) will happen if a person wishes to be a cyber promoter and cyber expert.

- The categories under which content can be labelled ‘unlawful’ seems very vague and subject to interpretation. This can lead to people resorting to using this portal to score political or personal scores.
- This can lead to online vigilantism and make citizens spy on one another.
- This may cause a surveillance state to usher in.
- Social media platforms have become an effective forum for mobilisation, dissemination of views sometimes critical of the political parties in power, and an important platform for asserting individual autonomy and freedom of speech and expression enabled by access to the internet. Under this program, any statement or idea expressed on social media may be flagged by volunteers as unlawful.